POLICY PER LA GESTIONE DEL PHISHING

Il Consorzio del Giardino della Flora Appenninica riporta di seguito le regole da seguire nell'utilizzo della e-mail e nella gestione del phishing.

Il Consorzio del Giardino della Flora Appenninica dispone

1. PRESTARE ATTENZIONE AL MITTENTE

Il mittente può essere noto o sconosciuto. Se il mittente è sconosciuto occorre prestare attenzione e interrogarsi sulla ragione di tale contatto.

Il dipendente deve sempre interrogarsi sulla veridicità del contatto, evitando di aprire le e-mail inviate da contatti non noti, o da un'istituzione pubblica o da un ente bancario.

2. FARE ATTENZIONE ALLA GRAMMATICA DEL TESTO

Se il mittente è noto, prestare attenzione alle modalità di dialogo ed allertarsi se le stesse sono diverse da quelle utilizzate usualmente dall'interlocutore.

Analizzare il testo della mail, l'attenzione dovrebbe riversare soprattutto sui seguenti elementi:

i) messaggio inatteso;

il) testo generico;

ill testo pieno di errori di battitura o sintassi;

iv) testo tradotto da un'altra lingua;

v) ricevuto da altri mittenti (parenti, amici o colleghi di università o lavoro ...);

vi) contenuto istituzionale o ufficiale proveniente da Banca, Politico, Poste Italiane, Presidenti o Ex Presidenti, società di carte di credito, Google, Paypal ecc.;

vii) contenuto riguardante sanzioni, multe o addirittura richiesta di riscatti che chiedono di aprire un allegato o di inviare immediatamente i propri dati personali;

ix) testo troncato, senza una frase di chiusura;

×) testo minaccioso che mette ansia al lettore;

xi) contenuto entusiasmante che promette premi, vincite o occasioni della vita con un limite di tempo ristretto per portarlo ricevere;

Diffidare sempre da testi scritti in modo da provocare ansia e paranoia, non avere fretta nell'apertura della e-mail e non farsi prendere dal panico.

Generalmente, queste e-mail contengono un tono intimidatorio e allarmante. Altre volte, promettono premi e vincite. Diffidare dai messaggi che non vi identificano in modo certo, ma utilizzano un linguaggio generico "gentile utente" o "gentile cliente".

Spesso, il cyber criminale individua informazioni che riguardano la vita personale, quotidiana e lavorativa del destinatario per incardinare il messaggio proprio con specifiche informazioni che richiameranno la sua attenzione, come ad esempio: riferiti ad elementi contabili; provenienti dal corriere utilizzato; riferiti a fatture di un fornitore reale; provenienti dal dipartimento informatico dell'ente; provenienti da un servizio di cloud realmente utilizzato. E importante non fornire mai le informazioni richieste tramite la compilazione di un form, o scaricando un allegato o ancora cliccando sul contenuto della mail.

Se avete il serio dubbio che l'e-mail sia indirizzata a voi, contattate il mittente via telefono per accertarvi della veridicità del messaggio.

'utente potrebbe verificare l'indirizzo della mail analizzando l'header (intestazione)
attraverso gli strumenti predisposti dall'Azienda.

3. NON FORNIRE MAI INFORMAZIONI RIGUARDANTI CODICI E PASSWORD VIA MAIL.

Il dipendente non dovrebbe mai fornire codici personali o password via mail. Qualora per ragioni lavorative risulti essenziale la comunicazione di codici o identificativi, occorre innanzitutto verificare l'attendibilità della richiesta ed utilizzare gli strumenti di cifratura messi a disposizione. Nel caso risulti essenziale il dipendente è tenuto a riferirlo al ai vertici dell'ente con richiesta scritta.

Non fornire indicazioni attinenti le credenziali bancarie o messaggi che arrivano da società bancarie.

Generalmente, questi attacchi si avvalgono della medesima grafica, testo, colori, temi e persino URL e indirizzi web simili del sito produttore originale, contenenti comunicazioni legate a problematiche di malfunzionamento del sistema, ovvero, ad esempio:

i) problema con un pagamento;

ii) fattura o nota non pagata;

iii) abbonamento scaduto;

iv) multa da pagare;

v) blocco del servizio.

Qualora risulta necessario, occorre verificare la veridicità del mittente, utilizzare gli strumenti all'uopo predisposti e chiamare l'istituto bancario per accertarsi della richiesta.

4. FARE ATTENZIONE AGLI ALLEGATI

Prestare la massima attenzione nell'apertura degli allegati e non scaricarli se sussistono uno degli elementi sopra riportati.

5. FARE ATTENZIONE AI LINK PRESENTI NEL TESTO DELLA E-MAIL

Passare il mouse e leggere bene il link sottostante per verificare se vi sono elementi di allerta. Evitare di cliccare sui link contenuti nei messaggi di testo mail soprattutto se sussistono gli elementi sopra riportati.

6. ATTENZIONE ALLA PEC

La pec non è necessariamente un sistema di comunicazione elettronica sicura: la sua gestione segue, pertanto, le regole sopra riportate per l'e-mail.

7. NON TENERE IL SEGRETO

Nel caso in cui il dipendente fosse incorso in un attacco di phishing è suo dovere informare immediatamente il responsabile o in sua assenza il Titolare del trattamento.